East West University

Design and Implementation of Secured VPN of a Bank using Cisco Devices.

Prepared By:

Pradip Nath.

Abdullah Al Noman.

Department of Electronics and Communications Engineering.

East West University

Supervised By:

Professor Dr. M. Ruhul Amin.

Department of Electronics and Communications Engineering.

East West University

Declaration

Hereby we declare that this project report is an original piece of work carried out by us under the guidance and supervision of Prof. Dr. M. Ruhul Amin and Prof. Dr. Zahedul Hasan**”.** Also clarify that all of the submitted contents of this project are original in its figure, excluding those, which have been admitted specifically in thereferences. All the work process involved is from our own idea and creativity.

Signature of Supervisor **Signature of Authors**

Approval

The project Titled **"Design and Implementation of Secured VPN of a Bank using Cisco Devices"** has been submitted to the following board of examiners as a part of partial fulfillment of the requirement for the award of degree Bachelor of Science in Electronics and Communication Engineering on December 2015 by the following students and has been accepted as satisfactory.

Abdullah Al Noman.
ID : 2011-2-55-019

Pradip Nath .
ID : 2011-1-55-020

Supervisor

Professor Dr.M.Ruhul Amin.
Department of Electronics & Communications Engineering, East West University .

Co Supervisor

Dr. Md. Zahedul Hasan.
Chief Scientific Officer
Bangladesh Atomic Energy Commission
Adjunct Professor
Department of Electronics &Communications Engineering, East West University.

Chairperson

Dr. Gurudas Mandol.
Associate Professor
Department of Electronics & Communications Engineering , East West University .

Acknowledgement

We would like to express our gratitude and appreciation to all those who gave us the possibility to complete this Project. A special thanks to our Supervisor Prof. **Dr.M.RuhulAmin** whose help, suggestions and encouragement helped us to take our project especially on Networking.

We express our deepest thanks to our project co-supervisor Prof. **Dr.Zahedul Hasan** for his complete guidance and support. He supported to us by showing different method of information collection about the Project. He helped all time when we needed and he gave right direction toward completion of project.

We also want to thanks all faculty and staffs of Department of Electronics and Communication Engineering for their cooperation during full of support for the report completion, from the beginning till the end. Also thanks to all of our family members, friends and everyone, that have been contributed by supporting our work and help us during the project progress till it is fully completed.

Abstract

There is an increasing demand nowadays to connect to internal networks from distant locations. Employees often need to connect to internal private networks over the Internet (which is by nature insecure) from home, hotels, airports or from other external networks. Security becomes a major consideration when staff or business partners have constant access to internal networks from insecure external locations.

VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private “tunnel” to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet.

This paper provides a general overview of VPN and implementation over a Corporate company. We discuss the potential security risks as well as the security considerations that need to be taken into account when implementing a virtual private network.

Table of Contents

Chapter 1

Introduction

1.1 What is the Project is about

In today's interconnected world it is irrational to believe a computer network system is immune from an attacks or think of it as too small to be considered as a predator by intruders to gain whatever advantage they need. Sometimes company owners deceived by thinking that company's resource are not highly valued and hence, they are not worth to be targeted. The reality is even at this moment companies are losing a significant amount money and wealth because of negligence or lack of awareness about the security issues.

On the other hand smart leaders are taking steps not to be victims of globally-based cyber-attacks. Companies' Owners are spending a considerable amount of money to protect their resources and assets in order to achieve sustainable growth and stability on the course as desired. It is worth spending money and energy on asses' network vulnerability and to identify the possible threats that might cause damage to the current system and resources. This will help in developing an effective security policy that dictates what to do and by whom in the situation when a system is under an attack coming from inside or outside the company's premises. Hence these days it is absolutely necessary for companies to pay special attention to tightening their security layers to exist as companies and contest at the global level.

The purpose of this project is to design a Virtual Private Network (VPN) for a Bank and study the vulnerability of the system and implement security measures to protect network resources and system services.

Chapter 2

Description of the Bank and Necessity of Network Services

2.1 Background Information of the company:

City Bank Ltd. https://www.thecitybank.com/ is one of the best private commercial online Bank in Bangladesh . It is a top bank among the oldest five Commercial Banks in the country which started their operations in 1983. The Bank started They have many branches and lots of customer account for giving banking services . The bank currently has 87 online branches and 10 SME service centers, It currently has 46 ATMs of its own; and ATM sharing arrangement with a partner bank that has more than 550 ATMs in place; SMS Banking; Internet Banking and so on. The bank is also very active in the workers' foreign remittance business. It has strong tie-ups with major exchange companies in the Middle East, Europe, Far East & USA, from where thousands of individual remittances come to the country every month for disbursements through the bank's large network of 97 online branches. The company's aim is to add value in all areas of its involvement with customers for providing best services.

The aims and objectives of this project is that to design a secure VPN and the best method and solution of implementing a Virtual Private Network over City Bank Ltd. between its Head Office, Branch office and customer to access to various resources.

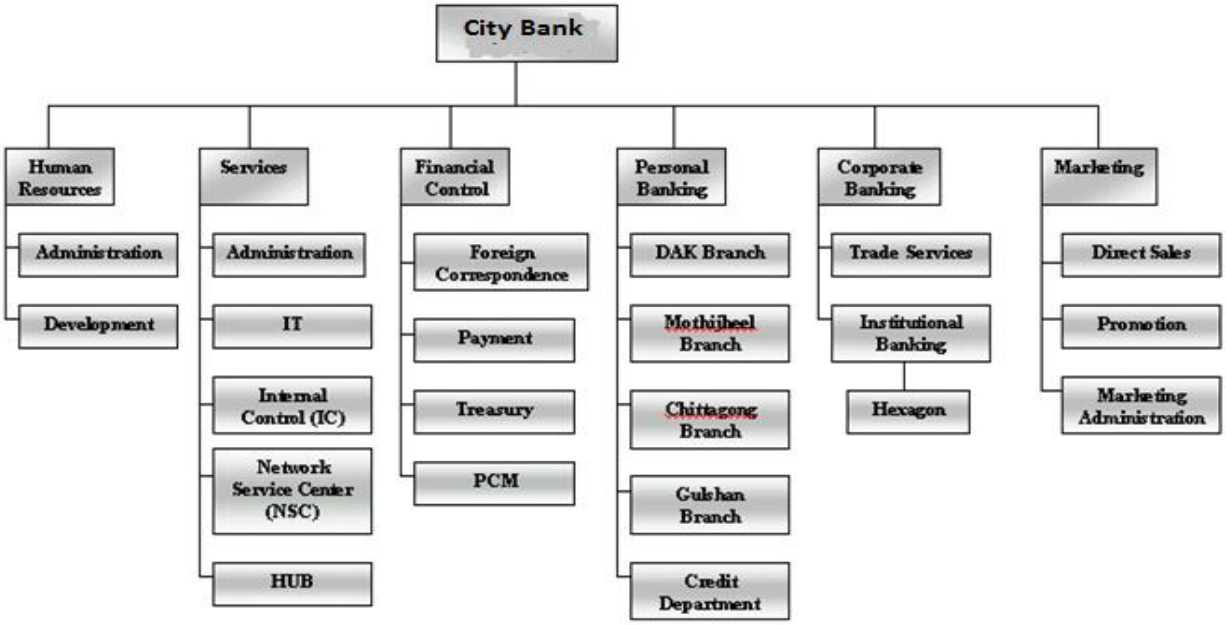


Figure 2.1 (a) : **City Bank system Operation diagram**

Figure 2.1(b) : Routing operation room

Figure 2.1 (b) : **Administration**

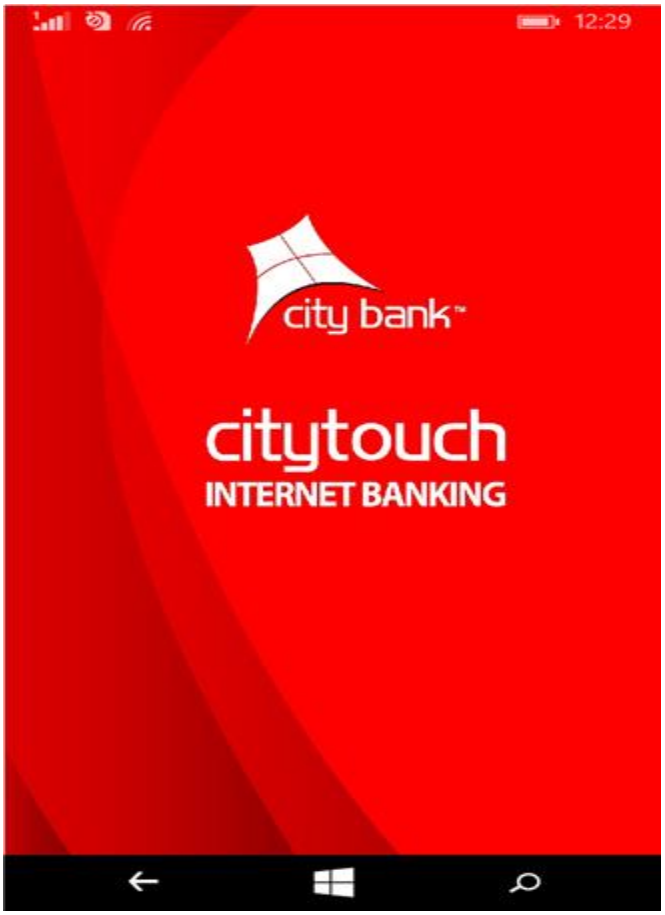


Figure 2(d) : i- banking

Necessity of Network Services :

The financial sector is among the most fast-paced and rapidly evolving verticals in today's global economy. Like most other industries, banking institutions of varying sizes rely heavily on network connectivity for handling some of their most critical and sensitive tasks. The ability to expand a customer base and generate new revenue streams smoothly and rapidly through ATM and local branch additions is imperative to enhancing market competitiveness in the banking sector. Bank networks must be able to rapidly scale to accommodate new secure links between banks and ATMs, regardless of location, and also provide infrastructure for interbank networking.

Self-service banking at ATMs

Many ATM machines are now fully connected service self-service channels that allow customers to pay bills, open new accounts, deposit checks, apply for loans or talk to virtual tellers. ATM branch requirements include a security element and a high availability element.

Online and Mobile Banking

Advancements in web technologies such as HTML5, CSS3 and JavaScript have seen more banks launching mobile web based services to complement native applications. Mobile banking is a system that allows customers of a financial institution to conduct a number of financial transactions through a mobile device such as a mobile phone or personal digital assistant. A recent study published by Mercator Advisory Group noted that customers—specifically smartphone and tablet owners—increasingly prefer self-service for banking. This ongoing shift in customer channel preference puts added importance on the reliability of network connectivity for banks as they compete for business and strive to boost customer satisfaction.

Retail banking

Of course, many consumers still prefer the tried-and-true model of doing their banking at a local branch. Today, many of these branches provide more than simple management of checking and savings accounts; they have expanded their offerings to include retirement planning, investment strategy, wealth management and more. For community retail banks, the

responsibility of keeping intruders from accessing confidential customer information is mandated by law. The network perimeter layer has historically been the focus of protecting a private network and is still essential for keeping intruders at bay and providing detection of possible intrusions. Adding these services means local branches require a scalable network infrastructure that can handle growing traffic and new applications.

Voice & Telephony Needs

Intra-office communications can be a major expense in banking, where voice communication is critical to continuity and enables faster service for customers. Private telephony networks that circumvent existing telephony networks and high international call rates can reduce expense. To ensure reliability and quality advanced CoS features that prevent VoIP calls from becoming compromised by other banking communications are needed

Data security

It's fairly obvious that financial information is incredibly sensitive, whether it belongs to a major financial corporation or a single individual. The financial sector faces robust regulatory requirements and the nearly constant threat of hackers, meaning a secure network solution is a necessity. As the amount of data being transferred continues to grow, so, too, will the importance of network security.

The banking sector requires a secure and reliable communication infrastructure to ensure operational efficiency. With widely distributed branches, local offices, and ATMs, often located in rural and remote areas lacking infrastructure, banking and financial organizations are turning to their own private networks as a preferred solution for connecting their dispersed locations under one core platform. In this environment of growing mobility, heightened competition and customer loyalty, that a gradual replacement of core banking systems is predicted to pick up again in coming years, as banking institutions are updating and replacing core banking systems and networks to improve their ability to compete in the new dawn of banking.

Information is now made easy with the availability of network communications. In a Bank for example, network communications plays an important part in keeping Customer account's database.

E-Banking

E-banking handles all types of banking transactions like account management, fund transfer and payments primarily over the internet. User can pay bills, check the account balance and transfer money to other parties, using e-banking facilities twenty four hours a day and seven days a week.

With e-banking, most of the transactions can be done at home or from the office, thus users save time on traveling and queuing at the bank counters.

Chapter 3

Overview of VPNs and Importance of VPN technologies

3.1 What is Virtual Private Network (VPN) ?

First of all, it is a **Network,** that is, it provides inter-connectivity to exchange information among various entities that belong to the VPN. Secondly it is **Private**, that is it has all the characteristics of a private network. "what characterizes a private network?" A private network supports a closed community of authorized users, allowing them to access various network-related services & resources. The final characteristic of a VPN is that it is **Virtua**l. A virtual topology is built upon an existing, shared physical network infrastructure. A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or

public networks like the Internet. A VPN enables to send data between two computers across link. The act of configuring & creating a virtual private network is known as virtual private Networking .

Hence, Virtual Private Network (VPN) is a network which uses a public network to transfer information using secure methods. This technology connects separate sites over the Internet and allows them to function as a single, private network. The information is sent through encrypted tunnels across the Internet but remain private during this transmission.[18]

3.2 Types of Virtual Private Network (VPN)

VPNs can be classified in a variety of ways.There are two types of VPN connections classification on Deployment.

- Site-to- Site VPN
- Remote-access VPN

3.2.1 Site-to-site VPN

A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world .

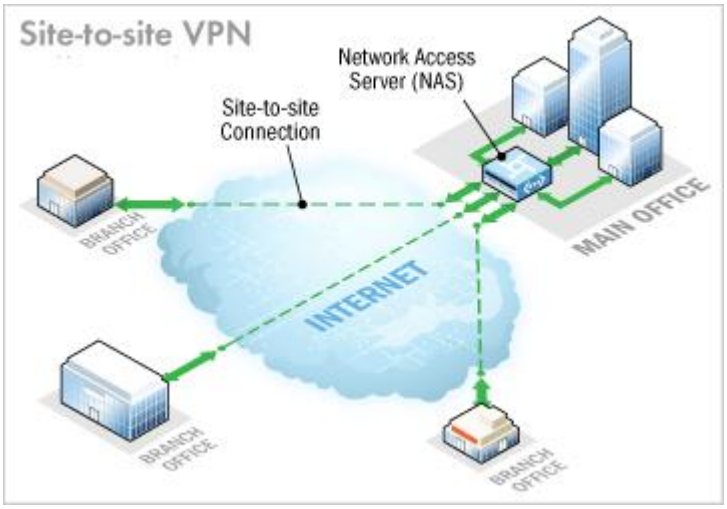


Figure 3.2.1(a): Site-to-Site VPN

There are two types of site-to-site VPNs:

- **Intranet-based** -- If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect each separate LAN to a single WAN.
- **Extranet-based** -- When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those companies' LANs. This extranet VPN allows the companies to work together in a secure, shared network environment while preventing access to their separate intranets.

Site-to-site VPN is used to connect geographically distributed corporate sites.

3.2.2 Remote-access VPN

A remote-access VPN allows individual users to establish secure connections with a remote computer network. Those users can access the secure resources on that network as if they were directly plugged in to the network's servers. An example of a company that needs a remote-access VPN is a large firm with hundreds of salespeople in the field. Another name for

this type of VPN is virtual private dial-up network (VPDN), acknowledging that in its earliest form, a remote-access VPN required dialing in to a server using an analog telephone system.

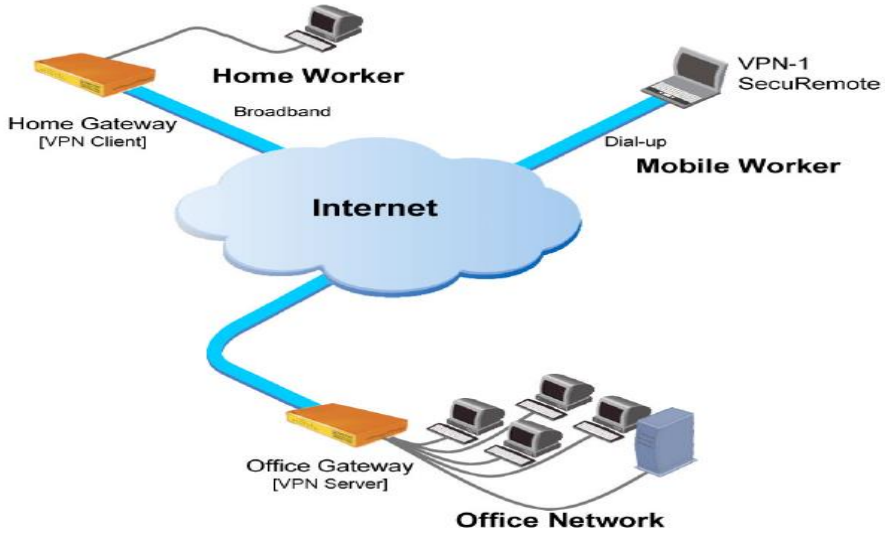


Figure 3.2.2(a): Remote Access VPN

There are two components required in a remote-access VPN. The first is a **network access server (NAS**), also called a media gateway or a remote-access server .

The other required component of remote-access VPNs is client software. In other words, employees who want to use the VPN from their computers require software on those computers that can establish and maintain a connection to the VPN. Most operating systems today have built-in software that can connect to remote-access VPNs, though some VPNs might require users to install a specific application instead. The client software sets up the tunneled connection to a NAS, which the user indicates by its Internet address. The software also manages the encryption required to keep the connection secure.

Large corporations or businesses with knowledgeable IT staff typically purchase, deploy and maintain their own remote-access VPNs. Businesses can also choose to outsource their remote-access VPN services through an enterprise service provider (ESP). A remote-access VPN is great for individual employees .

3.3 VPN Categories: Hardware and Software

There are two broad categories: hardware VPN systems and software VPN systems.

Most hardware VPN systems like the one in Figure 3.3 are encrypting routers that are secure and easy to use. Cisco 1900 Series Integrated Services Routers (ISR) are designed to meet the application demands of today's small branches and to evolve to cloud-based services. They

deliver virtualized applications and highly secure collaboration through the widest array of WAN connectivity at high performance that offers concurrent services at up to 25 Mbps. Hardware VPN systems provide the highest network throughput of all VPN systems. However, they may not be as flexible as software based systems.

Figure:3.3 Cisco 1900 Series Integrated Services Routers (ISR)

Software VPNs offer flexibility that hardware VPNs cannot. They are ideal in situations where both endpoints of the VPN are not controlled by the same organization as is the case in extranets. Software VPNs offers the most flexibility in how network traffic is managed. Many software products allow traffic to be tunneled based on address or protocol, unlike hardware products, which generally tunnel all traffic they handle, regardless of protocol. In situations where users are connecting over dial-up links, software VPNs may be the best choice because dialup does not require high performance and data throughput. Software systems are generally harder to manage than encrypting routers. They require knowledge of the VPN host operating system, the VPN software itself, and the security mechanisms of the organization. In business security perspective many VPN softwares are available with the license.

NETGEAR®

Netgear VPNG01L-20000S ProSafe VPN Client Professional - License - 1 user - electronic - Win
by Netgear

$77.00 new (3 offers)

3.4 Advantages :

VPN was not the first technology to make remote connections. Several years ago, the most common way to connect computers between multiple offices was by using a leased line. Leased lines, such as ISDN (integrated services digital network, 128 Kbps), are private network connections that a telecommunications company could lease to its customers. But it has more difficulties than VPN .

3.4.1 The Cost of Virtual Private Networks

When a company decides to transfer from a remote access server to a virtual private network, it should first and foremost consider the financial impact of the decision. If there is an opportunity to save money, then VPNs should definitely be considered an option.

One of the main cost concerns hinges on whether the virtual private network will be housed on site or outsourced to an independent service provider. When a business decides to use an outside provider, it is immediately eliminating any costs for purchasing and maintaining the necessary equipment. The most the business will have to do is maintain security measures (usually a firewall) as well as provide the servers that will help authenticate users. Of course, this too can be done by an outside provider for an additional price. Outsourcing also cuts down on the number of employees that would be required to manage and maintain the virtual private network.

Today, there are a greater number of providers who help companies service their virtual private networks than ever before. This has forced many of the providers to be more competitive and therefore develop the communication and management skills necessary to keep their customers happy. This in turn has led to better all around service for the companies who decide to outsource their VPNs.

There are several disadvantages to outsourcing virtual private networks. There is an obvious loss of control when an outside provider is running things. Remote users that are in different cities, states, or even countries may also experience difficulty dialing in to the VPN. Several roaming services are available to help eliminate this problem, but they can often be costly solutions.

If a business decides to run a virtual private network in house, it is looking at larger startup costs upfront because the proper equipment must be purchased and a trained staff must be

hired to maintain it. The advantage is that once this is done, the company has more control over features like authentication and access. A large corporation may find this more beneficial than a small business because it may already have the staff in place to take on such a project. Still, the potential for retraining the staff to properly operate the VPN exists, and this is another cost that should be considered.

3.4.2 VPN and Security

Virtual private network systems are constantly evolving and becoming more secure through four main features: tunneling, authentication, encryption, and access control. These features work separately, but combine to deliver a higher level of security while at the same time allowing all users (including those from remote locations) to access the VPN more easily.

Tunneling is what creates the connection between a user (either from a remote location or separate office) to the main LAN. This connection is called a tunnel and is essentially the circuit-like path that transfers private information through the Internet (which is a public forum). This requires a corporate address to be programmed into the dial-up network to ensure privacy.

To avoid crowded connections, a tunneling feature called "switching" was developed. This feature helps differentiate between direct and remote users to determine which connections should receive the highest priority. The switching can either be programmed directly into the virtual private network or upgraded so that the hardware recognizes each connection on an individual basis.

Incoming callers to the virtual private network are identified and approved for access through features called authentication and access control. These features are usually set up by the IT manager who enters a user's individual identification code or password into the main server, which cuts down on the chances that the network can manipulated from outside the company. Authentication also offers the chance to regulate access to the material on the LAN so that select users can only view certain information.

Encryption is the security measure that allows information on a virtual private network to be scrambled so that it becomes meaningless to unauthorized users. Encrypted data is eventually unscrambled at the end of the tunnel by a user with the proper authorization. This process is usually done via a private IP address that encrypts the information before it leaves the LAN or a remote location.

Despite these precautions, some companies are still hesitant to transfer highly sensitive and private information over the Internet via a virtual private network and still resort to tried and true methods of communication for such data.[16]

3.4.3 Performance

Performance is second to security when evaluating the tunneling protocols for VPN. Performance is measured in terms of throughput and latency. Latency is essentially the communication delay, an expression of how much time it takes for a packet of data to get from one designated point to another. Encryption in a packet-based protocol further increases the latency, as the packets need to be reassembled in the correct order before decryption can occur.

QoS (Quality of Service) aims to ensure that your mission critical traffic has acceptable performance. In the real world where bandwidth is limited and diverse applications from videoconferencing to ERP database lookups must all strive for scarce resources, QoS becomes a vital tool to ensure that all applications can coexist and function at acceptable levels of performance.

Quality of Service (QOS) is a key component of any VPN service.[11]

3.4.4 VPN Network Scalability

The cost to an organization of building a dedicated private network may be reasonable at first but increases exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations, but 4 branch offices require 6 lines to directly connect them to each other, 6 branch offices need 15 lines, and so on.

Internet based VPNs avoid this scalability problem by simply tapping into the the public lines and network capability readily available. Particularly for remote and international locations, an Internet VPN offers superior reach and quality of service(Qos).

3.4.5 Virtual Private Networks and Small Business

The growing number of options as well as solutions that are more affordable make virtual private network technology that much more attractive to small business owners. Some VPN software is even available on a trial basis so that businesses can find the solution that works best for them. Another option would be ISPs and NSPs (network service providers), which are also starting to provide more VPN services at better rates.

3.4.6 Compatibility with Broadband Technology

VPNs allow mobile workers, telecommuters and day extenders to take advantage of high-speed, broadband connectivity, such as DSL and Cable, when gaining access to their corporate networks, providing workers significant flexibility and efficiency

Chapter 4

Security features of VPN

4.1 Firewalls

A firewall provides a strong barrier between your private network and the Internet. IT staff can set firewalls to restrict what type of traffic can pass through from the Internet onto a LAN, and on what TCP and UDP ports. Even without a VPN, a LAN should include a firewall to help protect against malicious Internet traffic.

A firewall works closely with a router program to filter network packets and then determine whether or not to forward these packets to their destination. By using Cisco's 1700 routers, which is a VPN product, they can be upgraded to include firewall capabilities. It is recommended that a good firewall be in place before incorporating the VPN technology into the existing network.

4.2 Authentication

Authentication is used to prevent access to the private network by outsiders of the organization. This is done either by password authentication (shared secret) which is widely used or digital certification (issued electronic document) vouching for an individual's identity. VPNs use a stronger from of authentication called multi-factor authentication. This form of authentication is based on utilizing something owned and known, making it more secure since it cannot be guessed or stolen as is the case for password authentication. Many VPNs are based on this concept and support SecurIP (Secure IP) by a token card Security Dynamics. SecurIP provides authenticated Web access. This token card combines secret key encryption with a one-time password, which is automatically generated by encrypting a timestamp with the secret key. This one-time password is valid for a short interval of about 30 to 60 seconds. The digital certification is highly used as an authentication method for VPNs, since it binds the identity of an individual to a public key. This means that the digital signal will contain the public key, information specific to the user and issuer, validity period as well as other management information. All this information is used in creating the encrypted message digest, using the certificate authority's private key to 'sign' the certificate. In turn, the two communicating parties mutually authenticate each other. The PKI (Public Key Infrastructure) is the set of technologies responsible for generating, managing and revoking public keys, private keys and certificates.

4.3 Encryption

A virtual private network (VPN) is only as good as its encryption capabilities. You could use encryption to protect files on your computer or e-mails you send to friends or colleagues. An encryption key tells the computer what computations to perform on data in order to encrypt or decrypt it. The most common forms of encryption are **symmetric-key** encryption **or public-key** encryption:

In symmetric-key encryption, all computers (or users) share the same key used to both encrypt and decrypt a message.

In public-key encryption, each computer (or user) has a public-private key pair. One computer uses its private key to encrypt a message, and another computer uses the corresponding public key to decrypt that message.[2]

4.4AAA Server

An AAA server is a server program that handles user requests for access to computer resources and, for an enterprise, provides authentication,authorization,and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.The current standard by which devices or applications communicate with an AAA server is the Remote Authentication Dial-In User Service (RADIUS).

4.5 Tunneling

Virtual private network technology is based on the idea of tunneling . Tunneling is the process of placing an entire packet within another packet before it's transported over the Internet. That outer packet protects the contents from public view and ensures that the packet moves within a virtual tunnel. This layering of packets is called encapsulation.

Figure : 4.5 (a) Tunneling in VPN

4.5.1 Types of Tunneling

Mainly supports two types of tunneling - **voluntary** and **compulsory**. Both types of tunneling are commonly used.

- **voluntary tunneling** In this tunneling ,The VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs).Then, the VPN client application creates the tunnel to a VPN server over this live connection.
- **Compusory tunneling** In compulsory tunneling, the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels. Compulsory VPN tunneling authenticates clients and associates them with specific VPN servers using logic built into the broker device.

4.5.2 Tunneling Protocols

VPN tunnels use one of four main networking protocols, which provide the sufficient level of security as shown below;[15]

4.5.2.1 PPTP (Point to Point tunneling protocol)

PPTP is a protocol or technology that supports the use of VPN's. Using PPTP, remote users can access their corporate networks securely using the Microsoft Windows Platforms and other PPP

(Point to Point tunneling Protocols) enabled systems. This is achieved with remote users dialing into their local internet security providers to connect securely to their networks via the internet.

PPTP has its issues and is considered as a weak security protocol according to many experts, although Microsoft continues to improve the use of PPTP and claims issues within PPTP have now been corrected. Although PPTP is easier to use and configure than IPSec, IPSec outweighs PPTP in other areas such as being more secure and a robust protocol.

4.5.2.2 L2TP (Layer 2 Tunneling Protocol)

L2TP is an extension of the PPTP (Point to point tunneling protocol), used by internet service providers to provide VPN services over the internet. L2TP combines the functionality of PPTP and L2F (Layer 2 forwarding protocol) with some additional functions using some of the IPSec functionality. Also L2TP can be used in conjunction with IPSec to provide encryption, authentication and integrity. IPSec is the way forward and is considered better than the layer 2 VPN's such as PPTP and L2TP**.**

4.5.2.3 IPSec (IP Security)

IPsec operates on layer 3 and so can protect any protocol that runs on top of IP.IPSec is a framework consisting of various protocols and algorithms which can be added to and developed. IPSec provides flexibility and strength in depth, and is an almost perfect solution for securing VPN's. The only drawback is IPSec requires setting up on the corporate network and on the client end and is a complex framework to work with. IPSec is used for both site to site and remote user connectivity**.**

4.5.2.4 SSL VPN (Secure Socket Layer)

provides excellent security for remote access users as well as ease of use. SSL is already heavily used such as when you shop online, accessing your bank account online, you will notice an SSL protected page when you see the "https" in your browser URL bar as opposed to "http". Using SSL VPN would mean thousands of end user's would be able to access the corporate network without the support of an administrator and possible hours of configuring and trouble shooting, unlike IPSec. The end user would just need to know the address of the SSL VPN portal. Another advantage is they can do this from any computer as they do not have to rely on a configured client side software.

Chapter 5

Design of VPN for the Bank and IP planning

5.1 VPN Design proposal

The City Bank has many branches in Bangladesh. The main office has an Email server and File server .Branches from different remote areas can easily communicate with each other and clients can check the account balance, money transanction and other online banking services.

The administrator of the branch sales office needs to configure a virtual private network (VPN) connection between the branch sales office and the corporate office to enable the remote connections.

Completing planning worksheets for VPN connection from the branch office to remote sales employees ,The administrator of the Head office create VPN design and IP planning worksheets to help configure virtual private network (VPN) between the branch sales office and the corporate office.

Here we designed both Site-to-Site and Remote-Access VPNs over City bank ltd. For secure connectivity.

Network requirement

- All the offices should be interconnected with each other using VPN technology.
- The users at all the location should be able to access the email,google and file server.
- Users at all the locations should have access to internet, and should not be routed through the VPN network.
- Appliances like routers to setup the network.
- Identify additional requirements like public ip addresses, internet connections etc.
- Identify the IP network schema for all the locations.
- Identify the methodology to route internet traffic separately and not through the tunnel.

- user must know whether the IP address assigned to the other VPN device is static or dynamic. If the other VPN device has a dynamic IP address .
- Remote Branch Offices must know the shared key (passphrase) for the tunnel. The same shared key must be used by each device.
- The encryption method used for the tunnel (DES, 3DES, AES-128 bit, AES-192 bit, or AES-256 bit). The VPN devices must use the same encryption method.
- Branch Offices must know the authentication method for each end of the tunnel(MD5 or SHA-1). The VPN devices must use the same authentication method to transfer information with Head office.

5.2 Site-to-Site VPN Design

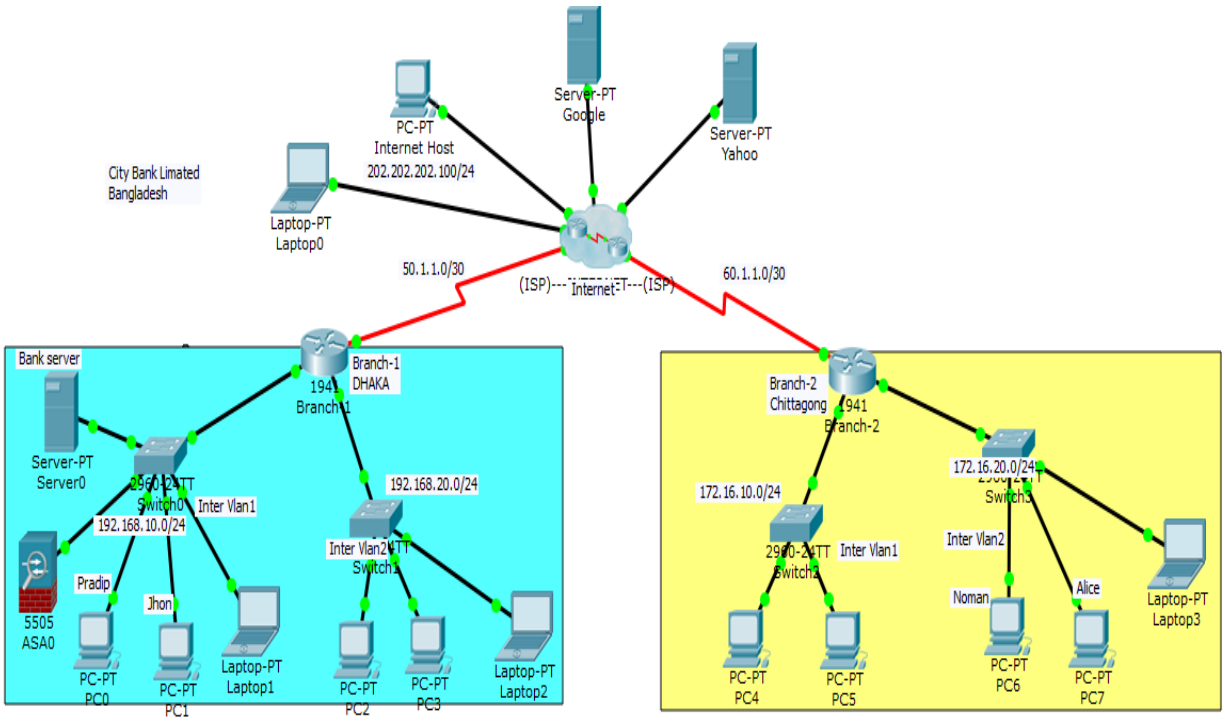


Figure 5.3 : site-to-site VPN for City Bank Ltd

Procedure:

City bank employee Noman wants to communicate with Pradip.

Stage 1: Noman establishes a TCP handshake with the VPN server and send First data packet

– Second packet send VPN server to the VPN client program

running on Noman's laptop

– Third packet: ack from client to VPN server

• **Stage 2**: authentication

– Client sends encrypted password and username to access VPN Server.However, VPN server CANNOT authenticate.

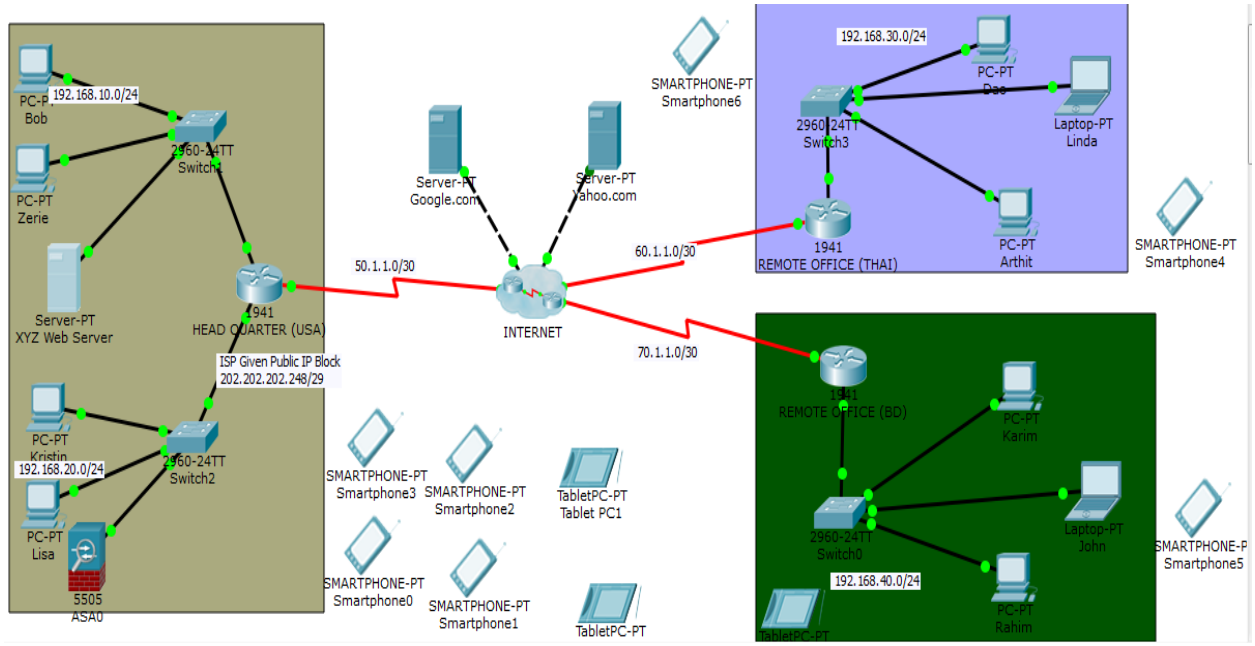
– So, VPN server forwards the password to the AAA server (through a separate TCP session)

– The AAA server checks the password

– The AAA server sends "YES" message to VPN server;in addition, AAA server will tell the VPN server that Noman has permission to access the real server.

– VPN server tells the client through the first TCP session that Noman is authenticated

5.3 Remote-Access VPN Design:



Procedure:

If the bank has branches throughout the world With growing numbers of individuals working remotely, telecommuting or traveling the bank needs to offer network connectivity to their data resources for users, regardless of the user's location. Employees, contractors, or partners may need to access the network when traveling or working from home or from other off-site locations. Then remote-access connectivity should support:

- User authentication—The AnyConnect client requires all remote-access users to authenticate before negotiating a secure connection. Both centralized authentication and local authentication options are supported.
- The remote access VPN is configured to provide different access policies depending on assigned user roles. User can easily access to internet but to enter data server user need to login with password and strong authentication.
- Strong encryption for data privacy—The Advanced Encryption Standard (**AES)** cipher with a key length of 256 bits is used for encrypting user data. Additional ciphers are also supported.
- The Secure Hash Standard 1 **(SHA-1**) cryptographic hash function with a 160-bit message digest is used to ensure that data has not been modified during transit.
- The Cisco **ASA** firewall supports between and the active and standby units of a resilient firewall pair in the event of a hardware failure.

5.4 IP Planning

5.4.1 Site-to-Site VPN IP Planning**:**

==========

- ***Branch-1(Dhaka Office):***

  - Inter VLAN-1 IP Planning:

Device	IP Address	Subnet Mask	Gateway	DNS Server
PC0	192.168.10.10/24	255.255.255.0	192.168.10.1	74.125.224.178
PC1	192.168.10.20/24	255.255.255.0	192.168.10.1	74.125.224.178
Laptop1	192.168.10.30/24	255.255.255.0	192.168.10.1	74.125.224.178
City Server	192.168.10.40/24	255.255.255.0	192.168.10.1	74.125.224.178

❖ Inter VLAN-2 IP Planning:

Device	IP Address	Subnet Mask	Gateway	DNS Server
PC2	192.168.20.10/24	255.255.255.0	192.168.20.1	74.125.224.178
PC3	192.168.20.20/24	255.255.255.0	192.168.20.1	74.125.224.178
Laptop2	192.168.10.30/24	255.255.255.0	192.168.20.1	74.125.224.178

❖ **Branch-1 DHAKA Router tunnel IP planning:**

IP Address:50.1.1.1/30
Subnet Mask:255.255.255.252
Serial port: sa0/0/0
Tunnel10 IP: 10.0.1.1/30

VPN Mode

Two tunnelling options when configuring site-to-site VPN:

Split tunnel: Send only site-to-site traffic, meaning that if a subnet is at a remote site, the traffic destined for that subnet is sent over the VPN. However, if traffic is destined for a network that is not in the VPN mesh the traffic is not sent over the VPN but instead is routed directly to the Internet from the local Router device.

Full tunnel: Send all traffic through a Full tunnel concentrator. In this mode, all Internet traffic will be routed via the chosen concentrator rather than going directly to the Internet. Mesh VPN peers are still accessible over direct VPN tunnels. You will need to specify which device is to act as the full tunnel concentrator.

Security features over full-tunnel VPN:

In a full tunnel topology, all security and content filtering must be performed on the full tunnel client. The full tunnel concentrator will not apply Content Filtering, IPS blocking, However, scanning will be performed for this traffic.

DNS Server,TFTPServer,FTP Server, AAA Server:

IP Address	Subnet Mask	Gateway
74.125.224.178	255.255.255.0	74.125.224.1

Yahoo server:

IP Address	Subnet Mask	Gateway	DNS Server
206.190.36.105	255.255.255.0	206.190.36.1	74.125.224.178

IT Host:

Device	IP Address	Subnet Mask	Gateway	DNS Server
Internet Host	202.202.202.100	255.255.255.0	202.202.202.1	74.125.224.178
laptop	DHCP	DHCP		

Branch-2(Chittagong Office):

- Inter VLAN-1 Ip Planning:

Device	IP Address	Subnet Mask	Gateway	DNS Server
PC4	172.16.10.10/24	255.255.255.0	172.16.10.1	74.125.224.178
PC5	172.16.10.20/24	255.255.255.0	172.16.10.1	74.125.224.178

- Inter VLAN-2 Ip Planning:

Device	IP Address	Subnet Mask	Gateway	DNS Server
PC6	172.16.20.10/24	255.255.255.0	172.16.20.1	74.125.224.178
PC7	DHCP	DHCP		
Laptop3	DHCP	DHCP		

❖ **Branch-2 Chittagong Router tunnel IP:**

IP Address: 60.1.1.1/30
Subnet Mask: 255.255.255.252
Serial port: sa0/0/1
Tunnel10 IP: 10.0.1.2/30

5.4.2 Remote Access VPN IP Planning:

==========

Head Quarter:

Device	IP Address	Subnet Mask	Gateway	DNS Server
Bob Pc	192.168.10.10/24	255.255.255.0	192.168.10.1	74.125.224.178
Zerie Pc	192.168.10.20/24	255.255.255.0	192.168.10.1	74.125.224.178
Bank Server	192.168.10.100/24	255.255.255.0	192.168.10.1	74.125.224.178
Kristin Pc	192.168.20.10/24	255.255.255.0	192.168.20.1	74.125.224.178

❖ **Head Quarter Router tunnel IP:**

IP Address: 50.1.1.1/30
Subnet Mask: 255.255.255.252
Serial port: sa0/0/0

DNS Server,TFTPServer,FTP Server, AAA Server:

IP Address	Subnet Mask	Gateway
74.125.224.178	255.255.255.0	74.125.224.1

Yahoo server:

IP Address	Subnet Mask	Gateway	DNS Server
206.190.36.105	255.255.255.0	206.190.36.1	74.125.224.178

Remote Office:

Device	IP Address	Subnet Mask	Gateway	DNS Server
Dao Pc	192.168.30.10/24	255.255.255.0	192.168.30.1	74.125.224.178
Linda	192.168.30.20/24	255.255.255.0	192.168.30.1	74.125.224.178
Arthit	192.168.30.30/24	255.255.255.0	192.168.30.1	74.125.224.178

Remote OfficeRouter tunnel IP :

IP Address: 60.1.1.1/30
Subnet Mask: 255.255.255.252
Serial port: sa0/0/0

Remote Office(BD):

Device	IP Address	Subnet Mask	Gateway	DNS Server
Karim	192.168.40.10/24	255.255.255.0	192.168.40.1	74.125.224.178
Johan	192.168.40.20/24	255.255.255.0	192.168.40.1	74.125.224.178
Arthit	192.168.40.30/24	255.255.255.0	192.168.40.1	74.125.224.178

Remote Office Router tunnel IP :

IP Address: 70.1.1.1/30
Subnet Mask: 255.255.255.252
Serial port: sa0/0/1

ISAKMP Phase 1 Policy Parameters

Parameters		Branch 1	Branch 2
Key distribution Method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption algorthim	DES, 3DES or AES	AES	AES
Hash algorthim	MD5 or SHA -1	SHA-1	SHA-1

Chapter 6
Implementation of VPN

6.1 Site-to-Site configuration

6.1.1 Step 1 :

CLI configuration:

Router CLI Configuration for Branch-1

```
==========================================

Branch-1#show running-config
Building configuration...


Current configuration : 1702 bytes
!version 15.1
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!hostname Branch-1
!ipcef
no ipv6 cef
!licenseudipid CISCO1941/K9 sn FTX15240000
license boot module c1900 technology-package securityk9
!cryptoisakmp policy 1
encraes 192
hash md5
authentication pre-share
group 5
!
cryptoisakmp key cisco address 60.1.1.1
!cryptoipsec transform-set TS esp-aes 256 esp-sha-hmac
!crypto map MyMap 10 ipsec-isakmp
set peer 60.1.1.1
set transform-set TS
match address MyAcl
!spanning-tree mode pvst
```

```
!interface Tunnel0
ip address 10.0.1.1 255.255.255.252
mtu 1476
tunnel source Serial0/0/0
tunnel destination 60.1.1.1
!interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
ipnat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.20.1 255.255.255.0
ipnat inside
duplex auto
speed auto
!
interface Serial0/0/0
ip address 50.1.1.1 255.255.255.252
ipnat outside
crypto map MyMap
!
interface Serial0/0/1
noip address
clock rate 2000000
shutdown
!
interface Vlan1
noip address
shutdown
!
routereigrp 100
network 192.168.10.0
network 192.168.20.0
network 10.0.1.0 0.0.0.3
!
ipnat inside source list SRC-DST interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!ip flow-export version 9
!
ip access-list extended MyAcl
permitip 192.168.0.0 0.0.255.255 172.16.0.0 0.0.255.255
ip access-list extended SRC-DST
denyip 192.168.0.0 0.0.255.255 172.16.0.0 0.0.255.255
permitip 192.168.0.0 0.0.255.255 any
!
```

```
line con 0
!line aux 0
!
linevty 0 4
login
!End
```

Verify tunnel prior to interesting traffic

Issue the show crypto IPsec sa Command on Branch-1. Notice that the number of packets encapsulated encrypted, DE-capsulated and decrypted are all set to 0.

```
Branch-1#show crypto ipsecsa

interface: Serial0/0/0
Crypto map tag: MyMap, local addr 50.1.1.1

protectedvrf: (none)
localident (addr/mask/prot/port):
(192.168.0.0/255.255.0.0/0/0)
remoteident (addr/mask/prot/port):
(172.16.0.0/255.255.0.0/0/0)
current_peer 60.1.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pktsencaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pktsdecaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pktscompr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 50.1.1.1, remote crypto
endpt.:60.1.1.1
pathmtu 1500, ipmtu 1500, ipmtuidb Serial0/0/0
     current outbound spi: 0x0(0)
```

Create interesting traffic:

```
Ping Pc-6 to Pc-2
```

Show crypto ipsecsa - Shows all current IPsec SAs at a peer:

```
interface: Serial0/0/0
Crypto map tag: MyMap, local addr 50.1.1.1
```

```
local crypto endpt.: 50.1.1.1, remote crypto
endpt.:60.1.1.1
pathmtu 1500, ipmtu 1500, ipmtuidb Serial0/0/0
current outbound spi: 0x0(0)

inboundespsas:
inbound ah sas:
inboundpcpsas:
outboundespsas:
```

Router CLI Configuration Branch-2

```
=======================================

Router#show running-config
Building configuration...

Current configuration : 1719 bytes
!
version 15.1
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostname Router
!ipcef
no ipv6 cef
!licenseudipid CISCO1941/K9 sn FTX152400000000
license boot module c1900 technology-package securityk9
!cryptoisakmp policy 1
encraes 192
hash md5
authentication pre-share
group 5
!
cryptoisakmp key cisco address 50.1.1.1
!
cryptoipsec transform-set TS esp-aes 256 esp-sha-hmac
!
crypto map MyMap 10 ipsec-isakmp
set peer 50.1.1.1
set transform-set TS
match address MyAcl
!
spanning-tree mode pvst
!
interface Tunnel0
```

```
ip address 10.0.1.2 255.255.255.252
mtu 1476
tunnel source Serial0/0/1
tunnel destination 50.1.1.1
!
interface GigabitEthernet0/0
ip address 172.16.10.1 255.255.255.0
ipnat inside
duplex auto
speed auto
interface GigabitEthernet0/1
ip address 172.16.20.1 255.255.255.0
ipnat inside
duplex auto
speed auto
!
interface Serial0/0/0
noip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
ip address 60.1.1.1 255.255.255.252
ipnat outside
crypto map MyMap
!interface Vlan1
noip address
shutdown
!routereigrp 100
network 172.16.10.0 0.0.0.255
network 172.16.20.0 0.0.0.255
network 10.0.1.0 0.0.0.3
!
ipnat inside source list SRC-DST interface Serial0/0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!ip flow-export version 9
!
ip access-list extended MyAcl
permitip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.255.255
ip access-list extended SRC-DST
denyip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.255.255
permitip 172.16.0.0 0.0.255.255 any
!
line con 0
!line aux 0
!
```

```
linevty 0 4
login
!
End
```

6.1.2 Step 2

Activation of security license

Configure Security License

Activation of security license is needed for site-to-site VPN configuration.Site-to-site VPN settings are accessible through the Security Appliance.

```
----------------------------

Branch-1(config)#license boot module c1900 technology-package
securityk9
Branch-1(config)#exit
Branch-1#write
Branch-1#reload
Branch-2(config)#license boot module c1900 technology-package
securityk9
Branch-2(config)#exit
Branch-2#write
Branch-2#reload
```

Define Interesting Traffic

Traffic is deemed interesting when the IPSec security policy configured in the IPSec peers starts the IKE process.

```
----------------------------
Branch-1(config)#ip access-list extended Router-Interesting-
Traffic
Branch-1(config-ext-nacl)#ip access-list extended MyAcl
Branch-1(config-ext-nacl)#permit ip 192.168.0.0 0.0.255.255
172.16.0.0 0.0.255.255
Branch-1(config-ext-nacl)#ip access-list extended SRC-DST
Branch-1(config-ext-nacl)#deny ip 192.168.0.0 0.0.255.255
172.16.0.0 0.0.255.255
Branch-1(config-ext-nacl)#permit ip 192.168.0.0 0.0.255.255 any
```

```
Branch-2(config)#ip access-list extended Router-Interesting-
Traffic
Branch-2(config-ext-nacl)#ip access-list extended MyAcl
Branch-2(config-ext-nacl)#permit ip 172.16.0.0 0.0.255.255
192.168.0.0 0.0.255.255
Branch-2(config-ext-nacl)#ip access-list extended SRC-DST
Branch-2(config-ext-nacl)#deny ip 172.16.0.0 0.0.255.255
192.168.0.0 0.0.255.255
Branch-2(config-ext-nacl)#permit ip 172.16.0.0 0.0.255.255 any
```

Modify NAT

A VPN tunnel cannot be established if both the destination network and the local network have the same subnets. The Apply NAT Policies feature or NAT over VPN is configured when both sides of a proposed site to site VPN configuration have identical, and hence overlapping, subnets.

```
------------
```

```
Router(config)#no ip access-list standard NAT-SOURCE
Router(config)#ip access-list extended NAT-SOURCE
Router(config-ext-nacl)#deny ip 172.16.1.0 0.0.0.255 172.16.2.0
0.0.0.63
Router(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#no ip access-list standard NAT-SOURCE
Router(config)#ip access-list extended NAT-SOURCE
Router(config-ext-nacl)#deny ip 172.16.2.0 0.0.0.63 172.16.1.0
0.0.0.255
Router(config-ext-nacl)#permit ip 172.16.2.0 0.0.0.63 any
Router(config-ext-nacl)#exit
```

Configure ISAKMP Phase I

As part of building an IPsec VPN gateway on a Cisco router, it's essential to implement ISAKMP policies using IKE to ensure secure VPN configuration.

```
---------------------------
```

```
Branch-1(config)#crypto isakmp policy 1
Branch-1(config-isakmp)#encraes 192
Branch-1(config-isakmp)#hash md5
Branch-1(config-isakmp)#authentication pre-share
Branch-1(config-isakmp)#group 5
Branch-1(config-isakmp)#lifetime 86400
Branch-1(config-isakmp)#exit
```

```
Branch-1(config)#crypto isakmp key cisco address 60.1.1.1
Branch-2(config)#crypto isakmp policy 1
Branch-2(config-isakmp)#encraes 192
Branch-2(config-isakmp)#hash md5
Branch-2(config-isakmp)#authentication pre-share
Branch-2(config-isakmp)#group 5
Branch-2(config-isakmp)#lifetime 86400
Branch-2(config-isakmp)#exit
Branch-2(config)#crypto isakmp key cisco address 50.1.1.1
```

Configure Phase 2

```
====================

Branch-1(config)#crypto ipsec transform-set TS esp-aes 256 esp-
sha-hmac

Branch-1(config)#crypto map MyMap 10 ipsec-isakmp
Branch-1(config-crypto-map)#match address Router-Interesting-
Traffic
Branch-1(config-crypto-map)#crypto map MyMap 10 ipsec-isakmp
Branch-1(config-crypto-map)#set peer 60.1.1.1
Branch-1(config-crypto-map)#set transform-set TS
Branch-1(config-crypto-map)#match address MyAcl
Branch-1(config-crypto-map)#exit

Branch-2(config)#crypto ipsec transform-set TS esp-aes 256 esp-
sha-hma
Branch-2(config)#crypto map MyMap 10 ipsec-isakmp
Branch-2(config-crypto-map)#set peer 50.1.1.1
Branch-2(config-crypto-map)#set transform-set TS
Branch-2(config-crypto-map)#match address MyAcl
Branch-2(config-crypto-map)#match address Router-Interesting-
Traffic

Router(config-crypto-map)#exit
```

Apply VPN MAP

VPN Maps is created in order to help users to find the best VPN server for their specific needs.

```
---------------

Branch-1(config)#int s0/0/0
Branch-1(config-if)#crypto map VPN-MAP

Branch-2(config)#int s0/0/1
Branch-2(config-if)#crypto map VPN-MAP
```

6.2Remote-access VPN implementation

6.2.1 Step 1

Router (USA Head Office)Configure

```
Router#sh running-config
Building configuration...

Current configuration : 2346 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!hostname Router
!aaa new-model
!aaa authentication login UAUTHEN local
!aaa authorization network GAUTHZ local
!no ip cef
!no ipv6 cef
!username hk secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username john secret 5 $1$mERr$neEIG6GcKrToz5/Gy.swa.
username linda secret 5 $1$mERr$D/zNiZIn/wbs6BKuL7DzY0
!license udi pid CISCO1941/K9 sn FTX1524KAU1
license boot module c1900 technology-package securityk9
!crypto isakmp policy 1
encr aes 192
authentication pre-share
group 5
!crypto isakmp client configuration group VPNCLIENT
key Cisco123
pool MYPOOL
netmask 255.255.255.0
!
crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
!
crypto dynamic-map DYNMAP 1
set transform-set TS
reverse-route
```

```
!
crypto map CLIENT-MAP client authentication list UAUTHEN
crypto map CLIENT-MAP isakmp authorization list GAUTHZ
crypto map CLIENT-MAP client configuration address respond
crypto map CLIENT-MAP 1 ipsec-isakmp dynamic DYNMAP
!
spanning-tree mode pvst
!
!
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface Serial0/0/0
ip address 50.1.1.1 255.255.255.252
ip nat outside
crypto map CLIENT-MAP
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip local pool MYPOOL 192.168.100.111 192.168.100.222
ip nat pool PUBLIC 202.202.202.249 202.202.202.253 netmask
255.255.255.248
ip nat inside source list SRC pool PUBLIC
ip nat inside source static 192.168.10.100 202.202.202.254
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.100.0
0.0.0.255
```

```
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.100.0
0.0.0.255
ip access-list extended SRC
deny ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.100.0 0.0.0.255
deny ip host 192.168.10.100 any
permit ip 192.168.10.0 0.0.0.255 any
permit ip 192.168.20.0 0.0.0.255 any
!
line con 0
!line aux 0
!
line vty 0 4
!
End
```

Router (THAI Branch)Configure

```
Router#sh running-config
Building configuration...

Current configuration : 1060 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
no ip cef
no ipv6 cef
!
!
license udi pid CISCO1941/K9 sn FTX1524KN0L
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.30.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
```

```
speed auto
shutdown
!
interface Serial0/0/0
ip address 60.1.1.1 255.255.255.252
ip nat outside
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list SRC interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
ip access-list extended SRC
deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
permit ip 192.168.30.0 0.0.0.255 any
!
line con 0
!line aux 0
!
line vty 0 4
login
!
End
```

Router (BD Branch)Configure

```
Building configuration...

Current configuration : 1060 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
!
```

```
no ip cef
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX1524BQA8
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.40.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
ip address 70.1.1.1 255.255.255.252
ip nat outside
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list SRC interface Serial0/0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!ip flow-export version 9
ip access-list extended SRC
deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
permit ip 192.168.40.0 0.0.0.255 any
!
line con 0
line aux 0
!
line vty 0 4
login
End
```

6.2.2 Step 2

Configuration Head Quarter (USA)

```
========================
HEADQUARTER(config)#aaa new-model
HEADQUARTER(config)#aaa authentication login UAUTHEN local
HEADQUARTER(config)#aaa authorization network GAUTHZ local

HEADQUARTER(config)#username hk secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
HEADQUARTER(config)#username john secret 5
$1$mERr$neEIG6GcKrToz5/Gy.swa.
HEADQUARTER(config)#username linda secret 5
$1$mERr$D/zNiZIn/wbs6BKuL7DzY0
HEADQUARTER(config)#

HEADQUARTER(config)#license boot module c1900 technology-package
securityk9


HEADQUARTER(config)#crypto isakmp policy 1
HEADQUARTER(config-isakmp)#encr aes 192
HEADQUARTER(config-isakmp)#authentication pre-share
HEADQUARTER(config-isakmp)#group 5
HEADQUARTER(config-isakmp)#

HEADQUARTER(config-isakmp)#crypto isakmp client configuration
group VPNCLIENT
HEADQUARTER(config-isakmp-group)#key Cisco123
A key already exists for groupVPNCLIENT
HEADQUARTER(config-isakmp-group)#pool MYPOOL
HEADQUARTER(config-isakmp-group)#netmask 255.255.255.0
HEADQUARTER(config-isakmp-group)#exit

HEADQUARTER(config)#crypto ipsec transform-set TS esp-aes 256
esp-sha-hmac
HEADQUARTER(config)#crypto dynamic-map DYNMAP 1
HEADQUARTER(config-crypto-map)#set transform-set TS
HEADQUARTER(config-crypto-map)#reverse-route

HEADQUARTER(config-crypto-map)#crypto map CLIENT-MAP client
authentication list UAUTHEN
HEADQUARTER(config)#crypto map CLIENT-MAP isakmp authorization
list GAUTHZ
HEADQUARTER(config)#crypto map CLIENT-MAP client configuration
address respond
```

```
HEADQUARTER(config)#crypto map CLIENT-MAP 1 ipsec-isakmp dynamic
DYNMAP

HEADQUARTER(config)#spanning-tree mode pvst
HEADQUARTER(config)#interface GigabitEthernet0/0
HEADQUARTER(config-if)#ip address 192.168.10.1 255.255.255.0
HEADQUARTER(config-if)#ip nat inside
HEADQUARTER(config-if)#duplex auto
HEADQUARTER(config-if)#speed auto

HEADQUARTER(config)#interface GigabitEthernet0/1
HEADQUARTER(config-if)#ip address 192.168.20.1 255.255.255.0
HEADQUARTER(config-if)#ip nat inside
HEADQUARTER(config-if)#duplex auto
HEADQUARTER(config-if)#speed auto
HEADQUARTER(config-if)#exit

HEADQUARTER(config)#interface Serial0/0/0
HEADQUARTER(config-if)#ip address 50.1.1.1 255.255.255.252
HEADQUARTER(config-if)#ip nat outside
HEADQUARTER(config-if)#crypto map CLIENT-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
HEADQUARTER(config-if)#ex

HEADQUARTER(config)#interface Serial0/0/1
HEADQUARTER(config-if)#no ip address
HEADQUARTER(config-if)#clock rate 2000000
HEADQUARTER(config-if)#shutdown
HEADQUARTER(config-if)#exit

HEADQUARTER(config)#interface Vlan1
HEADQUARTER(config-if)#no ip address
HEADQUARTER(config-if)#shutdown
HEADQUARTER(config-if)#exit

HEADQUARTER(config)#ip local pool MYPOOL 192.168.100.111
192.168.100.222
%IP address range overlaps with pool: MYPOOL
HEADQUARTER(config)#ip nat pool PUBLIC 202.202.202.249
202.202.202.253 netmask 255.255.255.248
HEADQUARTER(config)#ip nat inside source list SRC pool PUBLIC
HEADQUARTER(config)#ip nat inside source static 192.168.10.100
202.202.202.254
HEADQUARTER(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/0
HEADQUARTER(config)#ip flow-export version 9
```

```
HEADQUARTER(config-ext-nacl)#access-list 101 permit ip
192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255
HEADQUARTER(config)#access-list 101 permit ip 192.168.20.0
0.0.0.255 192.168.100.0 0.0.0.255
HEADQUARTER(config)#ip access-list extended SRC
HEADQUARTER(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255
192.168.100.0 0.0.0.255
HEADQUARTER(config-ext-nacl)#deny ip 192.168.20.0 0.0.0.255
192.168.100.0 0.0.0.255
HEADQUARTER(config-ext-nacl)#deny ip host 192.168.10.100 any
HEADQUARTER(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255
any
HEADQUARTER(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255
any
```

Chapter 7

Result And Discussion

7.1 Test the VPN Connection

This section explains how to start and test implementing VPN connection.

After finishing configuration both systems and have successfully started the connection, should test the connectivity to ensure that the remote hosts can communicate with each other.

it will not be able to test and use VPN connection from within the internal network that we want to connect to. In order to test our connection, will need to connect from a different location. For example, if we are setting up a VPN connection to office, test it from home network, test it from an Internet cafe, or other side.

Following these steps in order to creat Tunnel and connectivity :

After intall Cisco ASDM Launcher. Enter the IP address for the interface you configured with the http - command. Also, enter a username and password .

Figure 7.1(a) :Cisco ASDM Launcher

Specify the outside IP address of the remote peer. Enter the authentication information to use, which is the pre-shared key in this picture. Click Next.

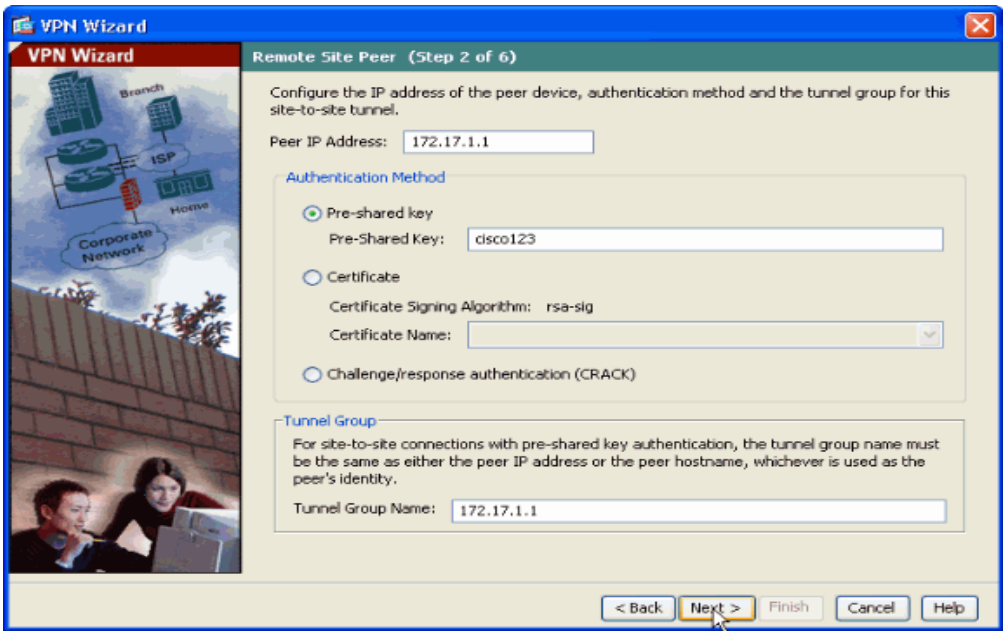


Figure 7.1 (b): VPN Wizard

Specify the attributes to use for IKE, also known as Phase 1. These attributes must be the same on both the ASA and the IOS Router. Click Next.

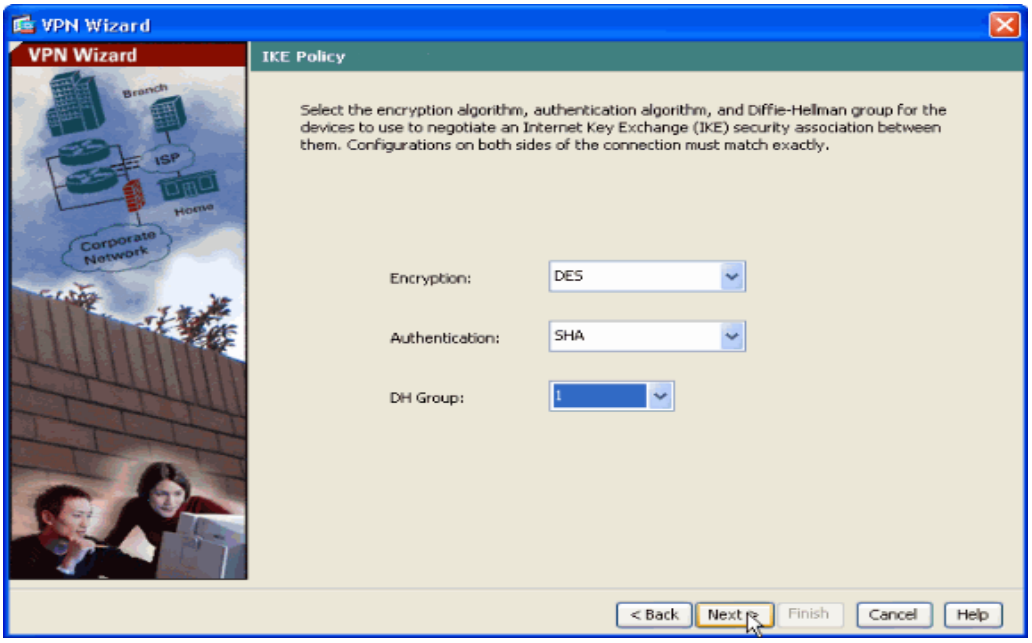


Figure 7.1 (b) : VPN wizard IKE

Specify the attributes to use for IPsec, also known as Phase 2. These attributes must match on both the ASA and the IOS Router

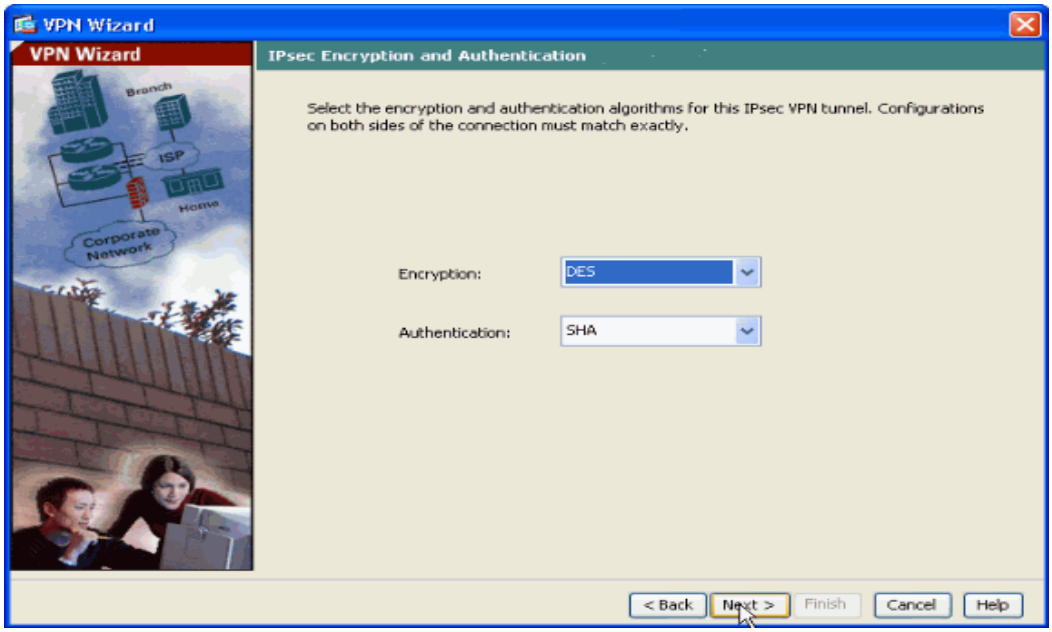


Figure 7.1 (c) :VPN wizard IPsec and Authentication

Choose the Local Network address, and click OK**.**

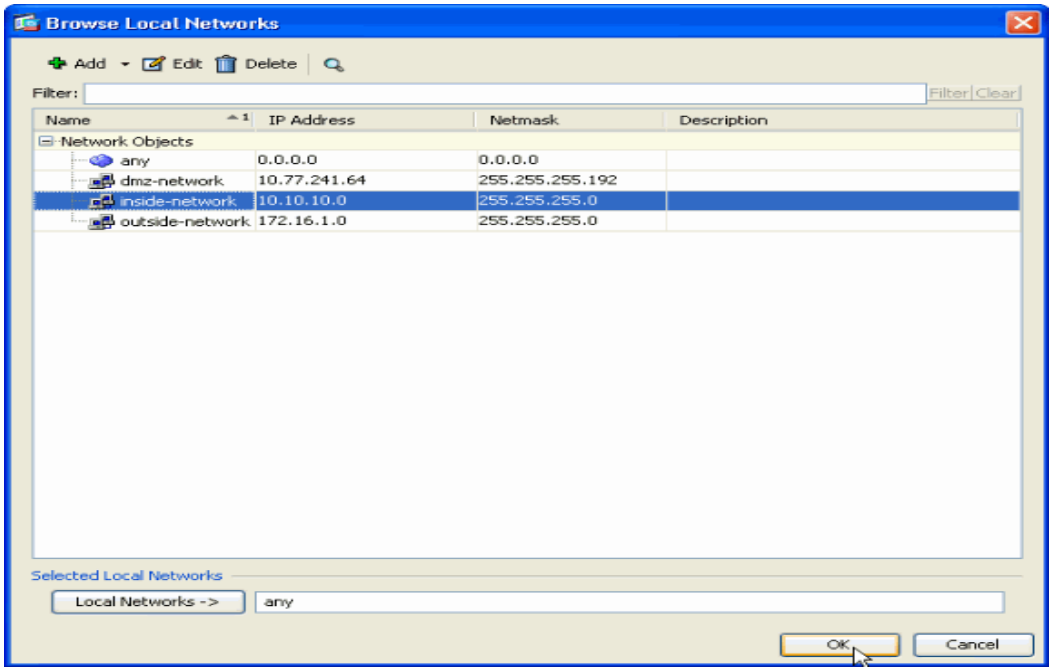


Figure7.1(d) : Test local network

7.2 Troubleshooting

Branch office VPN tunnels require a reliable connection and matching VPN configuration settings on both VPN endpoints. A configuration error or network connectivity issue can cause problems for branch office VPN tunnels to communicate head office**.**

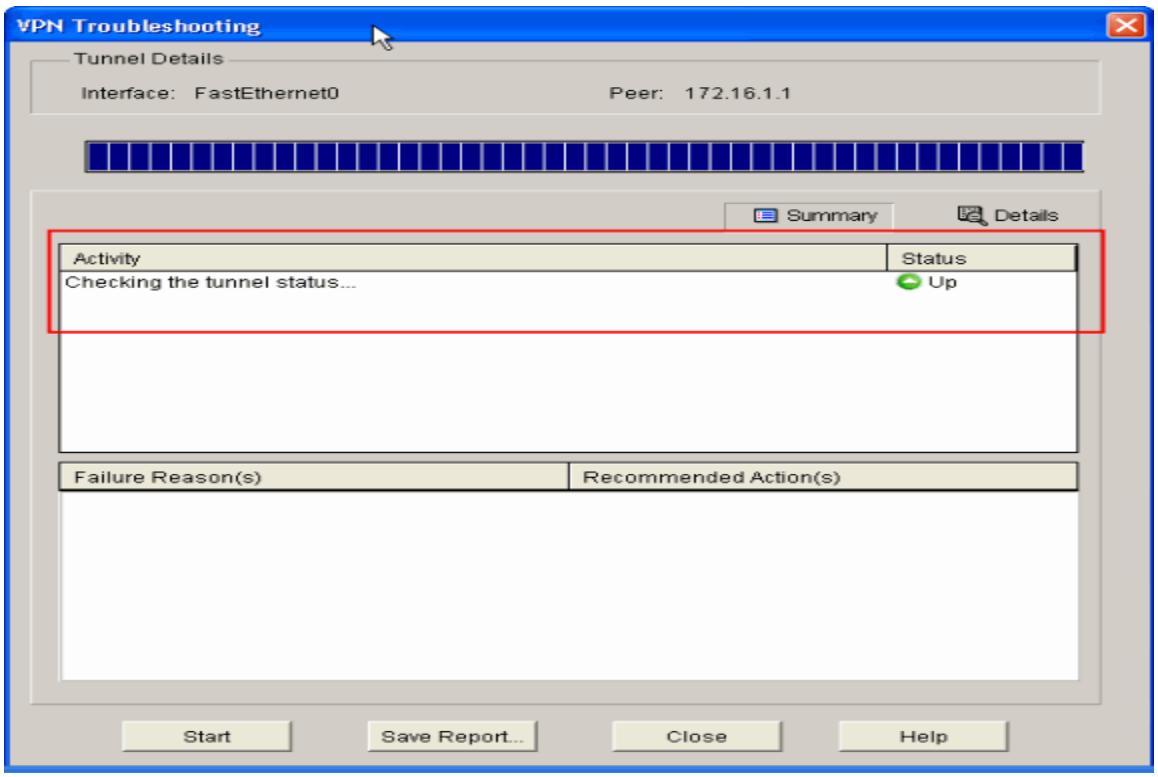


Figure : 7.2 Network connectivity Error

To troubleshoot the cause of a branch office VPN tunnel problem, we recommend that you should check up following issues.

* **Find out who is affected**

The first step in troubleshooting any VPN problem is to determine who is affected by it. That information can go a long way toward helping you figure out where to start looking for the problem. For example, if everyone in the company is having problems, then might look for a hardware failure on user VPN server, an incorrect firewall rule, or perhaps a configuration problem on VPN server.

* **Check to see whether users can establish VPN connectivity**

When user begin the actual troubleshooting process, start by determining whether the affected users can establish VPN connectivity. Not all VPN problems involve connection failures. Sometimes, users can connect, but they can't access network resources.

* **Look for policies preventing connectivity**

If you find that certain users are having trouble establishing connectivity, have them try to log in from a known good machine. If that doesn't work, there may be a policy in place preventing them from logging in.

*** Don't rule out the client**

If only a single user is affected by the problem and has no trouble logging in from another computer, the problem is most likely related to the computer that he or she was trying to connect from.

*** Try logging in locally**

This probably sounds silly, but when users tell me that they are having trouble logging in to the VPN, one of the first things I do is verify that they can log in locally.

* **See if affected users are behind NAT firewalls**

Another thing to check is whether affected users are connecting from computers that are behind a NAT firewall. Normally, NAT firewalls aren't a problem. However, some older firewalls don't work properly with VPN connections.

* **Check for Network Access Protection issues**

Microsoft created the Network Access Protection feature as a way for administrators to protect network resources against remote users whose computers are not configured in a secure manner. Although Network Access Protection (NAP) works well, it has been known to cause problems for end users.

* **Try accessing various network resources**

If users can log in to the VPN but they can't do anything once they're connected, the next step is to systematically attempt to connect to various resources on the network. This is important because user may find that some network segments are accessible while others are not.

*** Test connecting to resources by IP address rather than server name**

users can also try connecting to network resources by their IP address instead of by their name. If can access previously inaccessible resources by using IP addresses,that a DNS problem is to blame. If that happens,user should check to see which DNS server VPN clients are configured to use.

Chapter 8

Conclusion

VPN is an emerging technology that has come a long way. From an insecure break off of Public Telephone networks to a powerful business aid that uses the Internet as its gateway. VPN's technology is still developing, and this is a great advantage to businesses, which need to have technology that is able to scale and grow along with them. With VPN Company now have alternative benefits to offer to their employees, employees can work from home, take care of children while still doing productive, and have access work related information at anytime. VPN will also help to make the possibility of a business expanding its services over long distances and globally, more of a reality.

.

References

1) http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/112153-ccp-vpn-asa-router-config-00.html.
2) https://en.wikipedia.org/wiki/Virtual_private_network.
3) VPN Tunnel Configuration and policies , http://www.watchguard.com.
4) http://kb.cyberoam.com/default.asp?id=2310.
5) http://sumac.com/how-to-setup-a-vpn-to-access-your-office-files-remotely/.
6) http://www.informit.com/library/content.aspx?b=Troubleshooting_VPNs&seqNum=8
7) Bradley Mitchell, Introduction to VPN,
8) http://compnetworking.about.com/library/weekly/aa010701c.htm.
9) http://vpn.shmoo.com/vpn/FAQ.html#Q4.
10) "VPN Installation for remote sites" http://www.vpnazure.net.
11) "Performance of Virtual Private" Network http://www.techrepublic.com.
12) Eurescom: P1107 – IP Virtual Private Networks, PIR 3.3: Interworking of Security Technologies,February 2002.
13) Venkateswaran, R., "Virtual Private Networks", IEEE Potentials Magazine,February/March 2001.
14) Aboba, B. and G. Zorn, "Implementation of PPTP/L2TP Compulsory Tunneling via RADIUS",April 2000.
15) Microsoft White Paper, "Microsoft Privacy Protected Network Access: http://www.microsoft.com
16) Virtual Private Networking and Intranet Security", May 1999.
17) Brown, S., "Implementing Virtual Private Networks", McGraw Hill, 1999.
18) Ferguson & Huston. (1998, April). What is a VPN? Retrieved September 19, 2002, from http://www.employees.org/~ferguson/vpn.pdf